

PCT

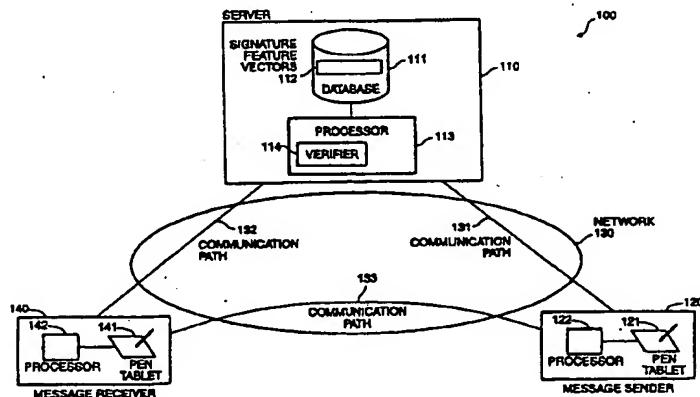
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|-----------|--|
| (51) International Patent Classification 6 : H04L 9/08 | A1 | (11) International Publication Number: WO 97/08868 (43) International Publication Date: 6 March 1997 (06.03.97) |
| (21) International Application Number: PCT/US96/13736 | | (81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). |
| (22) International Filing Date: 20 August 1996 (20.08.96) | | |
| (30) Priority Data: 08/519,430 25 August 1995 (25.08.95) US | | Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i> |
| (71) Applicant: QUINTET, INC. [US/US]; Suite 101, 10670 North Tantau Boulevard, Cupertino, CA 95014 (US). | | |
| (72) Inventors: CHAN, Chih; 13301 Glen Brae Drive, San Jose, CA 95070 (US). MOUSSA, Mohamed, Ali; 1302 Nelson Way, Sunnyvale, CA 94087 (US). | | |
| (74) Agents: D'ALESSANDRO, Kenneth et al.; D'Alessandro & Ritchie, P.O. Box 640640, San Jose, CA 95164-0640 (US). | | |

(54) Title: METHOD OF SECURE COMMUNICATION USING SIGNATURE VERIFICATION



(57) Abstract

A method and system for secure communication using signature verification. A message sender transmits to a trusted server a set of biometric data, such as representing the sender's handwritten signature, and a set of information about a message, such as a message identifier. The server verifies the sender's signature against a signature feature vector database, and provides the sender with a key for securely encoding the message. The sender encodes the message and transmits it to a message receiver. The receiver transmits to the server a second set of biometric data, such as representing the receiver's handwritten signature. The server verifies the receiver's signature against the signature feature vector database, and provides the receiver with the message identifier and a key for decoding the message. The biometric data represents a handwritten signature given contemporaneously by the sender or receiver, and is verified against a set of template signatures earlier given by the sender and receiver and recorded by the server, or may represent fingerprints, voiceprints, retinal images, other biometric data, or any arbitrary data which is particular to the sender or receiver and which the server is capable of verifying. The message comprises a single set of binary or text data, such as a file, or the message may comprise a stream of data and the method may be used for a virtual circuit to be created between the sender and receiver. The server may enhance the communication channel between the sender and the receiver, for example by transmitting signals to the sender representing whether the message was received.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|----|--------------------------|----|--|----|--------------------------|
| AM | Armenia | GB | United Kingdom | MW | Malawi |
| AT | Austria | GE | Georgia | MX | Mexico |
| AU | Australia | GN | Guinea | NE | Niger |
| BB | Barbados | GR | Greece | NL | Netherlands |
| BE | Belgium | HU | Hungary | NO | Norway |
| BF | Burkina Faso | IE | Ireland | NZ | New Zealand |
| BG | Bulgaria | IT | Italy | PL | Poland |
| BJ | Benin | JP | Japan | PT | Portugal |
| BR | Brazil | KE | Kenya | RO | Romania |
| BY | Belarus | KG | Kyrgyzstan | RU | Russian Federation |
| CA | Canada | KP | Democratic People's Republic of Korea | SD | Sudan |
| CF | Central African Republic | KR | Republic of Korea | SE | Sweden |
| CG | Congo | KZ | Kazakhstan | SG | Singapore |
| CH | Switzerland | LJ | Liechtenstein | SI | Slovenia |
| CI | Côte d'Ivoire | LK | Sri Lanka | SK | Slovakia |
| CM | Cameroon | LR | Liberia | SN | Senegal |
| CN | China | LT | Lithuania | SZ | Swaziland |
| CS | Czechoslovakia | LU | Luxembourg | TD | Chad |
| CZ | Czech Republic | LV | Latvia | TG | Togo |
| DE | Germany | MC | Monaco | TJ | Tajikistan |
| DK | Denmark | MD | Republic of Moldova | TT | Trinidad and Tobago |
| EE | Estonia | MG | Madagascar | UA | Ukraine |
| ES | Spain | ML | Mali | UG | Uganda |
| FI | Finland | MN | Mongolia | US | United States of America |
| FR | France | MR | Mauritania | UZ | Uzbekistan |
| GA | Gabon | | | VN | Viet Nam |

Title of the Invention

Method of Secure Communication Using Signature Verification

Background of the Invention**5 1. Field of the Invention**

This invention relates to a method of secure communication using signature verification.

2. Description of Related Art

In some environments, communicating messages is brought with the risk that 10 unauthorized persons may intercept the messages and read them, or may insert counterfeit messages into the message stream. Various methods have been proposed for communication in such environments; these various methods generally require message encryption and secure distribution of encryption keys.

In environments where communicating users are mobile, one problem which 15 has arisen in the art is the difficulty of easily and quickly authenticating the identities of users. One known solution is to provide each user with a password or other key, and to require the user to enter that password for authentication. However, this known method is subject to several drawbacks. First, the password may be forgotten or otherwise lost. This would require the user to obtain a new password or otherwise obtain authentication using another 20 channel.

Second, the password (or some transformation thereof) must be transmitted from the user's new position to some entity for authentication. This creates a point of attack for unauthorized persons to identify the password or its transformation and copy that information for their own use. Once a password has been compromised, it is easy for an unauthorized 25 person to enter that password and obtain improper authentication.

Third, the password may simply be guessed by unauthorized persons, particularly those who are familiar with the user.

Accordingly, it would be advantageous to provide a system in which users may easily and quickly authenticate their identities and communicate with other users, and in which it 30 is difficult for authentication means (1) to become lost, (2) to be copied by unauthorized persons, or (3) to be guessed by unauthorized persons.

Summary of the Invention

The invention provides a method of and system for secure communication using signature verification. A message sender transmits to a trusted server a set of biometric data, such as representing the sender's handwritten signature, and a set of information about a message, such as a message identifier. The server verifies the sender's signature against a signature feature vector database, and provides the sender with a key for securely encoding the message. The sender encodes the message and transmits it to a message receiver. The receiver transmits to the server a second set of biometric data, such as representing the receiver's handwritten signature. The server verifies the receiver's signature against the signature feature vector database, and provides the receiver with the message identifier and a key for decoding the message.

In a preferred embodiment, the biometric data represents a handwritten signature given contemporaneously by the sender or receiver, and is verified against a set of template signatures earlier given by the sender and receiver and recorded by the server. However, in alternative embodiments, the biometric data may represent facial images, fingerprints, hand images or handprints, foot images or footprints, human genome data, retinal images, voiceprints, recorded spoken statements, or other biometric data, or any arbitrary data which is particular to the sender or receiver and which the server is capable of verifying.

In a preferred embodiment, the message comprises a single set of binary or text data, such as a file. However, in alternative embodiments, the message may comprise a stream of data and the method may be used for a virtual circuit to be created between the sender and receiver. In other alternative embodiments, the server may enhance the communication channel between the sender and the receiver, for example by transmitting signals to the sender representing whether the message was received, and if so, when.

25

Brief Description of the Drawings

Figure 1 shows a block diagram of a system for secure communication using signature verification.

Figure 2 shows a flow diagram of a method of secure communication using signature verification using an arrangement as shown in figure 1.

Description of the Preferred Embodiment

In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. However, those skilled in the art would recognize, after perusal of this application, that embodiments of the invention may 5 be implemented using a set of general purpose computers operating under program control, and that modification of a set of general purpose computers to implement the process steps and data structures described herein would not require undue invention.

Secure Communication Using Signature Verification

Figure 1 shows a block diagram of a system for secure communication using 10 signature verification.

A system 100 for secure communication comprises a server 110, a message sender 120, a first communication path 131 between the server 110 and the sender 120, a message receiver 140, a second communication path 132 between the server 110 and the receiver 140, and a third communication path 133 between the sender 120 and the receiver 140.

15 In a preferred embodiment, the first communication path 131, the second communication path 132, and the third communication path 133 comprise communication paths in a network 130 such as a local area network (LAN), a wide area network (WAN), or a network of networks (an "internet"). Preferably, the first communication path 131, the second communication path 132, and the third communication path 133 comprise dynamically routed 20 communication paths constructed using network media, routers, and other intermediate processors in an internet. However, in alternative embodiments, the first communication path 131, the second communication path 132, and the third communication path 133 may comprise telephone connections in a telephone network, coupled between telephones at the server 110, the sender 120, and the receiver 140.

25 The server 110 comprises a database 111 of authentication information. The database 111 is preferably stored using a mass storage device such as magnetic disk, optical disk, or magnetic tape, but may alternatively be stored using any technique which allows for storage and retrieval of biometric information.

30 In a preferred embodiment, the database 111 comprises a set of signature feature vectors 112 such as those described with a method of signature verification shown in the following disclosures:

- o Application Serial No. 08/169,654, filed December 17, 1993, in the name of inventors Ali Mohamed Moussa and Chih Chan, titled "Method for Automatic Signature Verification", assigned to the same assignee, and having attorney docket number ACS-001; and
- o Application Serial No. 08/483,942, filed June 7, 1995, in the name of inventors Ali Mohamed Moussa and Chih Chan, titled "Method for Automatic Signature Verification", assigned to the same assignee, and having attorney docket number ACS-002.

5 Each of these applications is hereby incorporated by reference as if fully set forth herein. There are collectively referred to herein as the Signature Verification Disclosures.

10 However, in alternative embodiments, the database 111 may comprise alternative sets of biometric data or other data for validating signatures from the sender 120 or the receiver 140. For example, such biometric data may comprise all or a selected part of, or an encoding of, a set of biometric information about a person, which biometric information may comprise a facial image, a fingerprint, a hand image or handprint, a foot image or footprint, a human genome or related genetic information, a retinal image, a voiceprint or other record of a 15 spoken statement, or alternatively any other biometric information which is substantially unique to a first selected individual and difficult to adapt to a second selected individual. Biometric information differs from memorized information such as a password. Authentication using biometric information differs from physical forms of authentication such as using a pass key.

20 The server 110 also comprises a processor 113 operating under software program control for performing the functions described herein, having memory for storing software programs and data, and having mass storage for storing all or part of the database 111.

25 The processor 113 includes a verifier 114 for operating on the database 111 and on signature feature vectors 112 received from the sender 120 or the receiver 140. In a preferred embodiment, the verifier 114 performs the method of signature verification shown in the Signature Verification Disclosures. However, in alternative embodiments, the verifier 114 may perform another method of signature verification or verification of other biometric data.

The sender 120 comprises a pen tablet 121 for receiving a signature from the sending person. In a preferred embodiment, the pen tablet 121 comprises one like that shown in the Signature Verification Disclosures.

30 The sender 120 also comprises a processor 122 coupled to the pen tablet 121, operating under software program control for performing the functions described herein, having

memory for storing software programs and data, and for storing a signature feature vector 112 constructed for the sending person, and having mass storage for storing messages to be sent.

5 The receiver 140 comprises a pen tablet 141 for receiving a signature from the receiving person. In a preferred embodiment, the pen tablet 141 is similar to the pen tablet 121, and comprises one like that shown in the Signature Verification Disclosures.

The receiver 140 also comprises a processor 142 coupled to the pen tablet 141, operating under software program control for performing the functions described herein, having memory for storing software programs and data, and for storing a signature feature vector 112 constructed for the receiving person, and having mass storage for storing received messages.

10 The server 110, the sender 120, and the receiver 140 collectively perform the method shown herein.

Method Of Secure Communication

Figure 2 shows a flow diagram of a method of secure communication using signature verification using an arrangement as shown in figure 1.

15 At a flow point 200, the sender 120 desires to send a message to the receiver 140.

20 At a step 210, the sender 120 registers a set of signature feature vectors 112 for the sending person, using the first communication path 131 (between the server 110 and the sender 120). To perform this step 210, the sender 120 performs the step 211 through the step 213.

At a step 211, the sender 120 collects a set of template signatures from the sending person using the pen tablet 121.

25 At a step 212, the sender 120 forms a set of signature feature vectors 112 for the template signatures for the sending person, using the processor 122. The sender 120 preferably performs methods shown in the Signature Verification Disclosures.

At a step 213, the sender 120 transmits the set of signature feature vectors 112 for the template signatures for the sending person to the server 110, using the first communication path 131. In a preferred embodiment, it is not necessary that the first

communication path 131 is secure against reading by unauthorized third parties, only that the first communication path 131 is secure against unauthorized third parties altering the set of signature feature vectors 112 without detection.

Once the signature feature vectors 112 for the template signatures for the sending 5 person are registered at the server 110, the sending person may use the sender 120 to transmit a message. Although in a preferred embodiment, the signature feature vectors 112 for the template signatures for the sending person are transmitted from the sender 120 to the server 110, in alternative embodiments the sending person may deliver their signature feature vectors 112 by other means. For example, the sending person may alternatively use a different physical 10 device in place of the sender 120 for transmitting signature feature vectors 112 for their template signatures to the server 110, or may use the server 110 directly for entering their template signatures and forming signature feature vectors 112 therefor.

At a step 220, the sender 120 verifies a new signature from the sending person. To perform this step 220, the server 110 and sender 120 perform the step 221, the step 222, 15 and the step 223.

At a step 221, the sender 120 collects a test signature from the sending person using the pen tablet 121.

At a step 222, the sender 120 forms a signature feature vector 112 for the test 20 signature for the sending person. The sender 120 preferably performs methods shown in the Signature Verification Disclosures.

At a step 223, the server 110 receives the signature feature vector 112 for the test 25 signature for the sending person, and attempts to verify that test signature against the set of signature feature vectors 112 template signature for the sending person, using the processor 113. The server 110 preferably performs methods shown in the Signature Verification Disclosures.

If the attempt to verify is successful (i.e., the test signature is considered to match the template signatures), the server 110 proceeds with the step 230. If the attempt to verify is unsuccessful (i.e., the test signature is considered to not match the template signatures), the server 110 transmits a message so indicating to the sender 120.

30 In a preferred embodiment, if the attempt to verify is unsuccessful, the server 110 and the sender 120 may conduct a set of reattempts to verify the sending person, such as by

requesting an additional test signature and repeating the step 221, the step 222, and the step 223. Alternatively, the server 110 and the sender 120 may attempt to verify the sending person by other means, such as by using other biometric data, by using memorized data such as a password, or by using physical authentication such as requiring pass key from the sending person.

5

In a preferred embodiment, methods shown in the Signature Verification Disclosures are adapted to provide one of three alternative results from the attempt to verify the test signature -- (1) the test signature is considered to match the template signatures, (2) the test signature is considered to not match the template signatures, or (3) the result of the attempt to verify is considered ambiguous. In the event of the third alternative result, the server 110 and the sender 120 may conduct a supplemental attempt to authenticate the sending person, such as by requesting additional test signatures, by using other biometric data, by using memorized data such as a password, or by using physical authentication such as requiring pass key from the sending person.

10

15 At a step 230, the server 110 transmits to the sender 120 a key for encoding the message to be transmitted from the sender 120 to the receiver 140.

In a preferred embodiment, the key for encoding comprises a key for a symmetric encoding/decoding method such as the Data Encryption Standard (DES).

20

However, in alternative embodiments, the key for encoding may comprise a first key from a key pair used in a public key system.

At a step 240, the sender 120 encodes the message using the key for encoding, to generate an encoded message.

At a step 250, the sender 120 transmits the encoded message to the receiver 140 using the third communication path 133.

25

At a step 260, the receiver 140 registers a set of signature feature vectors 112 for the receiving person, using the second communication path 132 (between the server 110 and the receiver 140). To perform this step 260, the receiver 140 performs steps like the step 211 through the step 213. The receiver 140 collects a set of template signatures from the receiving person using the pen tablet 141. The receiver 140 forms a set of signature feature vectors 112 for the template signatures for the sending person, using the processor 142. The receiver 140

30

transmits the set of signature feature vectors 112 for the template signatures for the receiving person to the server 110, using the second communication path 132.

As was the case for the sending person, once the signature feature vectors 112 for the template signatures for the receiving person are registered at the server 110, the receiving 5 person may use the receiver 140 to receive a message. Although in a preferred embodiment, the signature feature vectors 112 for the template signatures for the receiving person are transmitted from the receiver 140 to the server 110, in alternative embodiments the receiving person may deliver their signature feature vectors 112 by other means similar to those shown herein for the sending person.

10 In addition, it is not necessary for the signature feature vectors 112 for the template signatures for the receiving person to be registered at the server 110, if they have already been registered at the server 110 for the same person as a sending person. Once an individual is registered at the server 110 in one capacity, the server 110 will retrieve their signature feature vectors 112 when they use the server 110 in another capacity.

15 At a step 270, the receiver 140 verifies a new signature from the receiving person. To perform this step 270, the receiver 140 performs steps like the step 221 through the step 223. The receiver 140 collects a test signature from the receiving person using the pen tablet 141. The receiver 140 forms a signature feature vector 112 for the test signature for the receiving person. The server 110 receives the signature feature vector 112 for the test signature 20 for the receiving person, and attempts to verify that test signature against the set of signature feature vectors 112 template signature for the receiving person, using the processor 113.

If the attempt to verify is successful (i.e., the test signature is considered to match the template signatures), the server 110 proceeds with the step 280. If the attempt to verify is unsuccessful (i.e., the test signature is considered to not match the template 25 signatures), the server 110 transmits a message so indicating to the receiver 140. If the attempt to verify is unsuccessful, the server 110 and the receiver 140 may conduct a set of reattempts to verify the receiving person, similar to processing in the step 223 for the sending person.

At a step 280, the server 110 transmits to the receiver 140 a key for decoding the encoded message that was transmitted from the sender 120 to the receiver 140.

30 In a preferred embodiment, the key for decoding comprises the same key as the key for encoding, for use in a symmetric encoding/decoding method such as the Data Encryption Standard (DES).

However, in alternative embodiments, the key for decoding may comprise a second key from a key pair used in a public key system, and corresponding to the key pair from which the key for encoding was selected.

In a preferred embodiment, server 110 generates a signal to the sender 120, 5 indicating that the receiver 140 has received the key for decoding, and therefore that biometric data for the receiving person has been verified. The server 110 transmits this signal to the sender 120 using the first communication path 131. This signal provides the sender 120 with an indication that the receiver 140 has received the message. Preferably, the signal provides an identifier for the message (so as to distinguish between several messages transmitted from the 10 sender 120 to the receiver 140) and a timestamp value representative of when the key for decoding was transmitted from the server 110 to the receiver 140.

At a step 290, the receiver 140 decodes the encoded message using the key for decoding, to recover the original message.

In a preferred embodiment, the message comprises a single set of binary or 15 text data, such as a file being transferred using a file transfer protocol or other network protocol. To generate the encoded message, the entire file is encoded using the key for encoding in a block encoding technique, thus creating an encoded file. The encoded file is transferred using the file transfer protocol or other network protocol. To recover the original message, the entire encoded file is decoded using the key for decoding.

20 However, in alternative embodiments, the message may comprise a stream of data and the method may be used for a virtual circuit to be created between the sender and receiver. To generate the encoded message, each separate transmission is encoded using the key for encoding in a stream encoding technique, thus creating an encoded stream of transmissions from the sender 120 to the receiver 140. The encoded stream is transferred using 25 a "telnet" protocol or other stream communication protocol. To recover the original stream of transmissions, the encoded stream is decoded using the key for decoding.

The receiver 140 may generate a response message to be transmitted to the sender 120. In this event, the receiver 140 may obtain a new key for encoding from the server 110, using the method described with regard to figure 2. Alternatively, since the receiver 120 30 has obtained from the server 110 a verification of the biometric data for the receiving person, the method may be streamlined for response messages from the receiver 140 to the sender 120. The server 110 may simply generate a key for encoding the response message and transmit that key for encoding to the receiver 140, and generate a key for decoding the response message and

transmit that key for decoding to the sender 120. In a preferred embodiment where the key for encoding and the key for decoding the original message are substantially identical, the receiver 140 may use the key for decoding the original message as a key for encoding the response message and the sender 120 may use the key for encoding the original message as a key for decoding the response message.

5

Alternative Embodiments

Although preferred embodiments are disclosed herein, many variations are possible which remain within the concept, scope, and spirit of the invention, and these variations would become clear to those skilled in the art after perusal of this application.

Claims

We claim:

1. A method for communication between a sender and a receiver, said method comprising
 - 5 transmitting from said sender to a server a set of biometric data for a sending person;
 - verifying, at said server, said biometric data for said sending person;
 - transmitting from said server to said sender a key for encoding said message;
 - encoding a message using said key for encoding to generate an encoded 10 message;
 - transmitting said encoded message to said receiver;
 - transmitting from said receiver to said server a set of biometric data for a receiving person;
 - verifying, at said server, said biometric data for a receiving person;
 - 15 transmitting from said server to said receiver a key for decoding said encoded message; and
 - decoding said encoded message at said receiver.
2. A method as in claim 1, comprising
 - encoding a second message using said key for encoding to generate a second 20 encoded message; and
 - decoding said second encoded message using said key for decoding.
3. A method as in claim 1, comprising
 - transmitting from said server to said receiver a key for encoding a response;
 - encoding a response using said key for encoding to generate an encoded 25 response; and
 - transmitting said encoded response to said sender;
 - transmitting from said server to said sender a key for decoding said encoded response; and
 - decoding said encoded response at said sender.
- 30 4. A method as in claim 1, comprising transmitting from said server to said sender a signal representing whether said biometric data for said receiving person was verified at said server.
5. A method as in claim 1, wherein said key for encoding said message and said key for decoding said encoded message are paired keys in a public key system.

6. A method as in claim 1, wherein said key for encoding said message and said key for decoding said encoded message are substantially identical.

7. A method as in claim 1, wherein said biometric data for said receiving person represents at least a portion of

- 5 a facial image,
- a fingerprint,
- a hand image,
- a handprint,
- a foot image,
- 10 a footprint,
- a human genome,
- a retinal image,
- a voiceprint, or
- a record of a spoken statement.

15 8. A method as in claim 1, wherein said biometric data for said receiving person represents a receiver's signature.

9. A method as in claim 1, wherein said step of verifying said biometric data for said receiving person comprises

- 20 receiving a set of template biometric data from said sender;
- receiving said biometric data for said receiving person; and
- comparing said biometric data for said receiving person against said set of template biometric data from said sender.

10. A system for communication between a sender and a receiver, said system comprising

- 25 an input device coupled to said sender, said input device disposed for receiving a set of biometric data for a sending person;
- a server, said server coupled to said sender and to said receiver, said server comprising a biometric data verifier and a generator of a key for encoding and a key for decoding;
- 30 means, at said sender, for encoding a message using said key for encoding, to generate an encoded message;
- a communication path between said sender and said receiver;
- an input device coupled to said receiver, said input device disposed for receiving a set of biometric data for a receiving person;

means, at said receiver, for decoding said encoded message using said key for decoding.

11. A system as in claim 10, comprising means, at said sender, for encoding a second message using said key for 5 encoding to generate a second encoded message; and means, at said receiver, for decoding said second encoded message using said key for decoding.
12. A system as in claim 10, comprising means, at said receiver, for encoding a response using said key for encoding to 10 generate an encoded response; and means, at said sender, for decoding said encoded response.
13. A system as in claim 10, comprising means, at said server, for transmitting to said sender a signal representing whether said biometric data for said receiving person was verified.
14. A system as in claim 10, wherein said key for encoding and said key for decoding are paired keys in a public key system.
15. A system as in claim 10, wherein said key for encoding and said key for decoding are substantially identical.
16. A system as in claim 10, wherein said biometric data for said 20 receiving person represents at least a portion of a facial image, a fingerprint, a hand image, a handprint, a foot image, a footprint, a human genome, a retinal image, a voiceprint, or 25 a record of a spoken statement.
- 30

17. A system as in claim 10, wherein said biometric data for said receiving person represents a receiver's signature.

18. A system as in claim 10, wherein said biometric data verifier comprises a set of template biometric data from a person whose biometric data is to be verified; and
5 means for comparing biometric data for said person against said set of template biometric data.

1/2

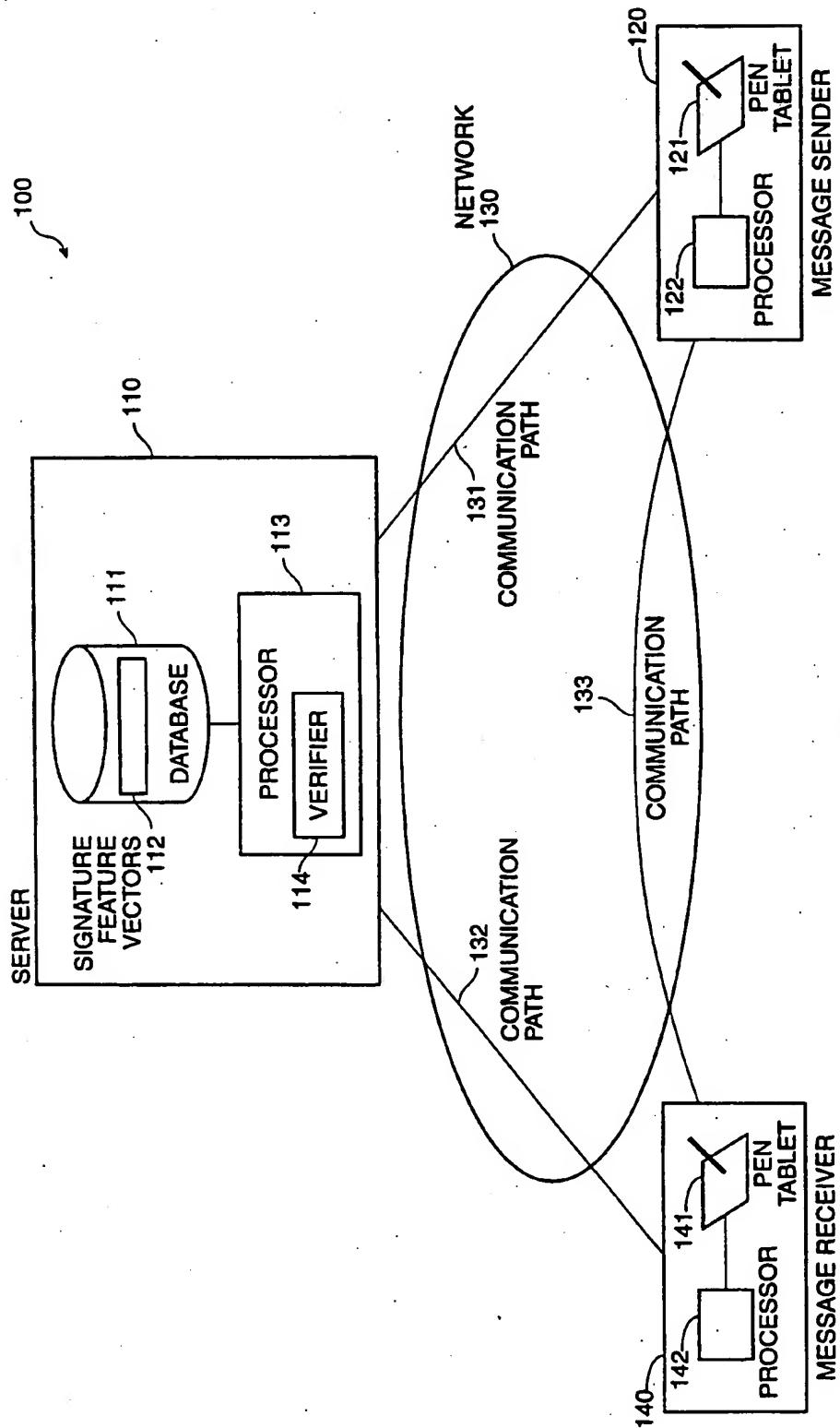


FIG. 1

SUBSTITUTE SHEET (RULE 26)

2/2

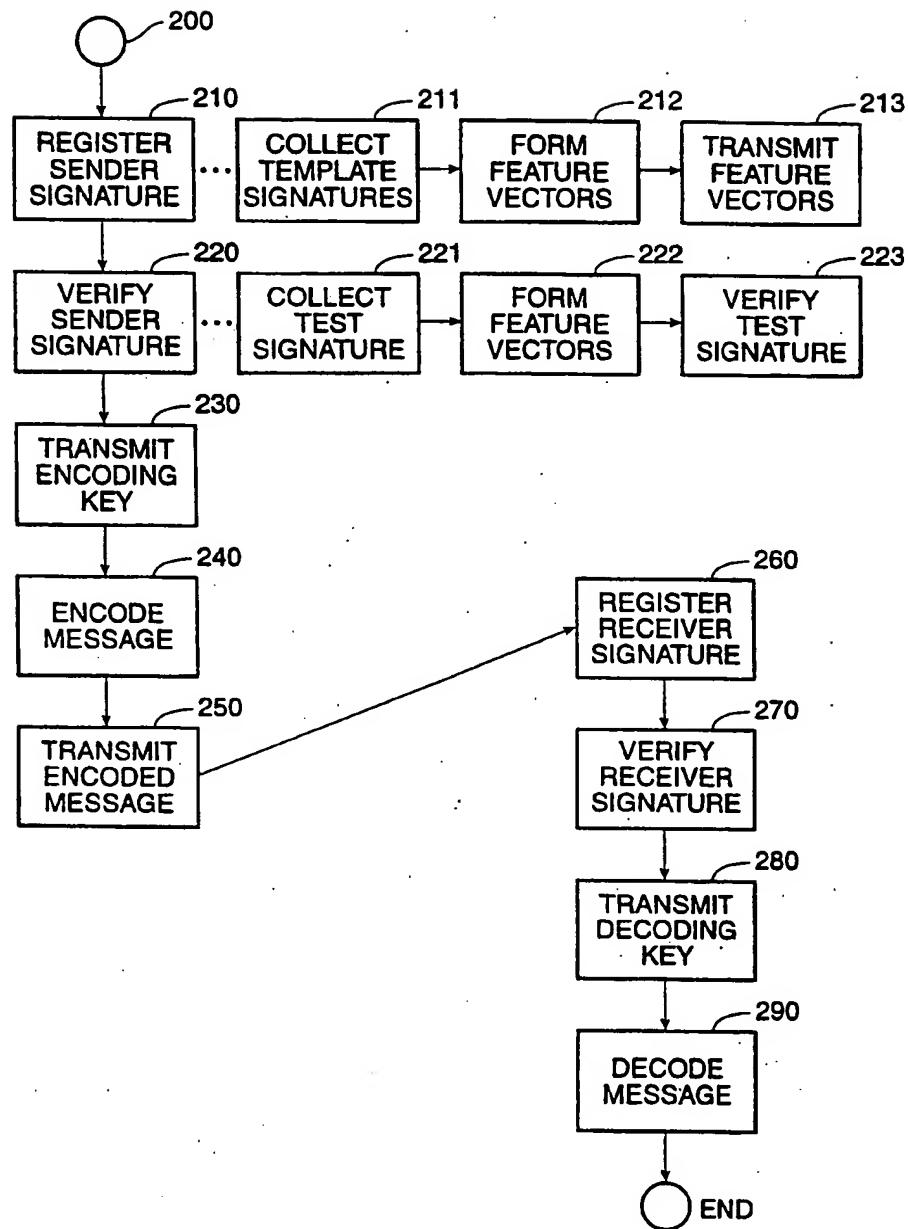


FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/13736

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|---|-----------------------|
| Y A | US,A,5 237 614 (WEISS) 17 August 1993 see column 1, line 43 - line 63 see column 2, line 59 - line 63 see column 3, line 51 - line 55 see column 9, line 20 - line 35 --- | 1,10 7,16 |
| Y A | EP,A,0 281 224 (HEWLETT-PACKARD) 7 September 1988 see page 1, line 15 - line 35 see page 4, line 50. - page 5, line 4 see page 7, line 29 - line 34 see page 10, line 3 - line 15 --- | 1,10 5,6,14, 15 |
| A | WO,A,95 16974 (QUINTET) 22 June 1995 cited in the application see abstract --- | 8,9,17, 18 |
| | -/- | |



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "V" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "A" document member of the same patent family

1 Date of the actual completion of the international search

18 December 1996

Date of mailing of the international search report

09.01.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentstaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

Intern. Application No.
PCT/US 96/13736

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|----------|--|-----------------------|
| A | US,A,4 993 068 (PIOSENKA ET AL.) 12 February 1991 see column 1, line 55 - column 2, line 5 see column 6, line 9 - line 14 see column 7, line 37 - column 8, line 47 ----- | 7,16 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

| | |
|------------------------------|--|
| International Application No | |
| PCT/US 96/13736 | |

| Patent document cited in search report | Publication date | Patent family member(s) | | Publication date |
|--|------------------|-------------------------|----------|------------------|
| US-A-5237614 | 17-08-93 | US-A- | 5485519 | 16-01-96 |
| | | US-A- | 5479512 | 26-12-95 |
| EP-A-281224 | 07-09-88 | DE-D- | 3888558 | 28-04-94 |
| | | DE-T- | 3888558 | 30-06-94 |
| | | JP-A- | 63226149 | 20-09-88 |
| | | US-A- | 4888800 | 19-12-89 |
| WO-A-9516974 | 22-06-95 | AU-A- | 1674795 | 03-07-95 |
| | | CA-A- | 2179302 | 22-06-95 |
| | | EP-A- | 0737342 | 16-10-96 |
| US-A-4993068 | 12-02-91 | NONE | | |